UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/575,424	04/10/2006	Yang Peng	CN 030035	3752

24737 7590 01/11/2010

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
01/11/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/575,424	PENG ET AL.	
	Examiner	Art Unit	
	JEFFREY D. POPHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20091007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 17-32 are pending.

Response to Arguments

1. Applicant's arguments filed 11/10/2009 have been fully considered but they are not persuasive.

Applicant argues that "the process of authenticating a server is not the same as authenticating content downloaded from a server." As explained in the previous office action, this is true of some authentication systems. For example, if a server is authenticated by sending a plaintext password to a client, and the client authenticates the server by a simple comparison of the password, then the password is authenticated, showing that the server has access to it. This is a very simple authentication mechanism that is not intended to authenticate any data other than the password itself. This system does authenticate the password (which is data), but does so without using a public key (the claims call for a public key to be used in authentication). However, Uranaka does not use this simple form of plaintext password for server authentication, and does not apply to the "the process of authenticating a server is not the same as authenticating content downloaded from a server" analysis, as will be explained below.

In Uranaka, the server signs data using its private key. Uranaka, column 15, lines 59-63 states that "the server 8 signs the double-encrypted AP-encrypting key

$e1(PK_u, R+e2(R, K_v))$

with a signing key or the server secret key SK_s after step 622." This clearly shows the server using its secret key to sign data (this data being the double-encrypted AP-encrypting key in this embodiment). The next sentence reads "While the client or DVD player 2 tests the signature by the server 8 with a test key or the server public key PK_s contained in the PK field 31 of the distribution descriptor 23 recorded in the burst cutting area of the DVD 2 before step 630." Therefore, the client will use the server public key to decrypt the signed double-encrypted AP-encrypting key. This has the dual effect of authenticating both the server and the double-encrypted AP-encrypting key. If the server is not authentic, only useless garbage will be obtained, as only the server could have encrypted the data properly using the server's secret key. If the server is authentic, then the specific server that owns that particular secret key will have signed the data, and the proper data (double-encrypted AP-encrypting key) will be obtained upon decryption and verification of the signature by the client/player. That is to say, in testing/verifying the signature, both authenticity of the data and authenticity of the server are obtained due to the fact that the server is only considered authentic if and only if the appropriate (authentic) data is obtained by decryption of the signature.

As one of ordinary skill in the art would realize, a signature provided by signing data with a private/secret key inherently provides authentication of both the data and the signer of the data upon proper verification/decryption using the public key corresponding to that particular private/secret key. If, upon decryption of the data using the public key, gibberish is obtained, then both the data and the

signer are considered unauthentic. However, if the signature is determined to be proper via such decryption, then both the data and the signer are considered authentic. Discussion regarding Schneier was provided in the last response to arguments in order to show what one of ordinary skill in the art would have known at the time of applicant's invention.

It is noted that the claims do not describe any other way for this authentication to ensue other than via the use of data that is signed by (or "added with", which is broader than signing) a secret/private key. Claim 20, for example, explicitly claims "a control system to verify the authenticity of the downloaded content using the public key read-out from the optical disk".

In the specification of the instant application, page 5, lines 12-19 describe how a piece of data is prepared for authentication. This paragraph reads, in part, "the downloaded contents are all authenticated. That is, when the optical disc content provider stores the content s corresponding to the optical disc on a web server, the optical disc content s provider itself or other CA (Certificate Authority, e.g. Internet Explorer of Microsoft and Navigator of Netscape, etc.) confirm that the contents are providable to the users and has been added with a Private key." As one can see here, the downloadable contents are "added with a Private key", such adding of a private key encompassing at least encrypting/signing data using the private key. This paragraph goes on to state that "Due to the presence of the Private key, the downloaded contents are not easy to be modified by others on the web." This sentence clearly states that, once encrypted (or added) with a private key, it is not easy to modify data. This is why the data can be verified as

authentic using the public key. If the data were to be modified after being encrypted with the private key, only garbage will be obtained upon decrypting the data with the public key, thereby failing the verification of authenticity. If, however, the data were not to be modified after being encrypted with the private key, the correct data will be obtained upon decryption with the public key, resulting in authentication of both the data and the entity that signed the data (as the entity that signed the data used the appropriate private key to sign the data).

This is exactly how Uranaka works. As described above, Uranaka encrypts the double-encrypted AP-encrypting key with the server's secret key in the signing step, and then verifies the signature using the public key, resulting in authentication of both the data and the server. The only way that the server of Uranaka can be authenticated is if the data itself is authentic.

Applicant argues that "If it is believed that this teaching is found in one or more other references, then these references should be made of record before being used in the rejection. As it stands, it is respectfully submitted that the Office Action has failed to point out in the prior art references of record the teaching of verifying "the authenticity of the downloaded content using the public key read-out from the optical disk" as for example recited in claim 20." First noted is that Schneier was only provided to show inherent properties/characteristics of signatures that one of ordinary skill in the art would have recognized at the time of applicant's invention. Second, Applicant does not appear to argue that the properties/characteristics of signatures described in Schneier are incorrect or irrelevant to Uranaka. Finally, Applicant provides no

argument against the fact that authenticating a server using the server's public key and a signature (formed by encrypting data with the server's private/secret key) inherently authenticates the data itself.

Claim Objections

2. Claims 20 and 32 are objected to because of the following informalities:

- Claim 20 has been amended to recite "the content residing on one or more computing devices distributed on a network". However, multiple instances of “content” have been set forth in the claim, including media content and content that is associated with the media content. It is unclear which of these is being referenced here. For purposes of prior art rejection, the above citation has been construed as “the content associated with the read out media content residing on one or more computing devices distributed on a network”.
- Claim 32 refers to “the optical disk player” which has not been set forth previously in claim 32 or claim 25 from which claim 32 depends. For purposes of prior art rejection, "the optical disk player" has been construed as "an optical disk player".
- Claim 32 has been amended to recite “playing the content in coordination with the content stored on the optical disk”. Previously, this portion of claim 32 read "playing the content stored on the optical disk in coordination with the downloaded content". As with claim 20, it is unclear which of the two pieces of content is being referred to with

respect to “the content”. Additionally, if the first instance of "the content" in this citation is meant to refer to the downloaded content, a new matter issue may be raised as was provided in the final office action dated 3/11/2009. For purposes of prior art rejection, “playing the content in coordination with the content stored on the optical disk” has been construed as “playing the media content stored on the optical disk in coordination with the downloaded content”, thereby fixing both potential issues.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 17, 18, 20, 22-25, and 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Uranaka (U.S. Patent 6,470,085) in view of Tsumagari (U.S. Patent Application Publication 2004/0126095).

Regarding Claim 20,

Uranaka discloses an optical disk player, comprising:

An optical disk driver unit to read out media content and a public key stored on an optical disk (Column 6, lines 42-54; Column

7, lines 19-33; Column 8, lines 34-41; and Column 12, lines 12-15; showing the makeup of the DVD player including DVD DRIVER, applications stored on the optical disk (applications defined as music, movies, games, etc. in column 4, line 66 to column 5, line 1), server public key stored on the disk, and reading of such data from the disk);

A network interface to download content associated with the read out media content, the content associated with the read out media content residing on one or more computing devices distributed on a network (Column 6, lines 42-58; Column 9, lines 30-46; and Column 9, line 61 to Column 10, line 20; showing the makeup of the DVD player including communication IF and interactions between the player and a server in order to download data associated with the content stored on the disk); and

A control system to verify the authenticity of the downloaded content using the public key read out from the optical disk before the read out media content is played (Figure 1, servers 8; Column 5, lines 20-42; Column 5, line 58 to Column 6, line 5; and Column 15, lines 57-67; showing authentication of the server and the downloaded data, as described above in the response to arguments);

But does not explicitly disclose that the read out media content is played in coordination with the associated downloaded content.

Tsumagari, however, discloses that the read out media content is played in coordination with the associated downloaded content (Paragraphs 43, 106, 116, 131, 156, and 174; showing downloading of ENAV contents from a server and playing of content from a DVD along with the ENAV contents). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the enhanced content system of Tsumagari into the content usage control system of Uranaka in order to allow the system to download enhanced data to supplement data stored on the optical disk, thereby ensuring that the player can always have the most up-to-date data without requiring a user to obtain a new disk.

Regarding Claim 17,

Claim 17 is a system claim that is broader than player claim 20 and is rejected for the same reasons.

Regarding Claim 25,

Claim 25 is a method claim that is broader than player claim 20 and is rejected for the same reasons.

Regarding Claim 22,

Uranaka as modified by Tsumagari discloses the player of claim 20, in addition, Tsumagari discloses that the downloaded content is an application program (Figure 10; and Paragraphs 143 and 167; ENAV contents comprising Java script for controlling reproduction of other ENAV contents, for example).

Regarding Claim 29,

Claim 29 is a method claim that is broader than player claim 22 and is rejected for the same reasons.

Regarding Claim 23,

Uranaka as modified by Tsumagari discloses the player of claim 22, in addition, Tsumagari discloses that the application program is a JAVA language application program (Figure 10; and Paragraphs 143 and 167, as just described).

Regarding Claim 30,

Claim 30 is a method claim that is broader than player claim 23 and is rejected for the same reasons.

Regarding Claim 24,

Uranaka as modified by Tsumagari discloses the player of claim 20, in addition, Uranaka discloses that the control system verifies the authenticity of the downloaded content by performing asymmetric cryptography using the public key stored on the optical disk and corresponding to a private key used to encrypt the downloaded content (Column 15, lines 57-67).

Regarding Claim 31,

Claim 31 is a method claim that is broader than player claim 24 and is rejected for the same reasons.

Regarding Claim 18,

Uranaka as modified by Tsumagari discloses the playing system of claim 17, in addition, Uranaka discloses that the public key is stored in a BCA zone of the optical disk (Figures 2 and 4; Column 5, lines 20-42; Column 5, line 58 to Column 6, line 5; and Column 8, lines 34-41).

Regarding Claim 32,

Uranaka as modified by Tsumagari discloses the method of claim 25, in addition, Uranaka discloses that the optical disk comprises digital information stored thereon, the stored digital information comprising:

Server information that is used by an optical disk player to download content for playing the optical disk (Figures 2 and 4; Column 5, lines 20-42; Column 5, line 58 to Column 6, line 5; and Column 15, lines 57-67); and

A public key that is used by the optical disk player to verify the authenticity of the downloaded content before playing the media content stored on the optical disk in coordination with the downloaded content (Figures 2 and 4; Column 5, lines 2-42;

Column 5, line 58 to Column 6, line 5; and Column 15, lines 57-67); and

Tsumagari discloses that the server information comprises a network address (Paragraph 39).

4. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Uranaka in view of Tsumagari, further in view of Ryan (U.S. Patent 5,754,648).

Uranaka as modified by Tsumagari does not explicitly disclose that the public key is stored in a media content zone of the optical disk.

Ryan, however, discloses that the public key is stored in a media content zone of the optical disk (Column 3, lines 47-67; and Column 8, lines 31-37). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the media security and tracking system of Ryan into the content usage control system of Uranaka as modified by Tsumagari in order to allow the system to provide additional authentication and authorization steps such that a device can ensure that both the disk and device are authentic and authorized for use with each other by using data stored on the optical disk itself and data stored on a magnetic track attached to the disk, thus decreasing the chance of unauthorized use thereof, and/or to provide the ability to track use of the media.

5. Claims 21 and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Uranaka in view of Tsumagari, further in view of Collins (U.S. Patent Application Publication 2002/0073316).

Regarding Claim 21,

Uranaka as modified by Tsumagari does not explicitly disclose that the control system detects whether the downloaded content is integral before verification, wherein the verification will not be executed if the downloaded content is detected to not be integral.

Collins, however, discloses that the control system detects whether the downloaded content is integral before verification, wherein the verification will not be executed if the downloaded content is detected to not be integral (Paragraphs 73-77; detecting whether the downloaded content is “integral” may comprise either, or both, verification of the program packet format and/or verification of the checksum, each of which must succeed before signature verification is performed). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the content authentication and access control system of Collins into the content usage control system of Uranaka as modified by Tsumagari in order to allow the system to detect when errors in the data have occurred, such that data with errors will not be allowed to be processed and only correct data will be

processed, and/or to ensure that the data is authentic before allowing access to proceed, thereby increasing security of the system by ensuring both integrity and authenticity of the content.

Regarding Claim 26,

Claim 26 is a method claim that is broader than player claim 21 and is rejected for the same reasons.

Regarding Claim 27,

Uranaka as modified by Tsumagari discloses that authentication of the downloaded content is performed prior to playing the read out media content in coordination with downloaded content (Uranaka, Column 15, lines 57-67, for example, as well as the discussion above with respect to playing in coordination), but does not explicitly disclose that the downloaded content will not be used if the downloaded content is not authenticated.

Collins, however, discloses that the downloaded content will not be used if the downloaded content is not authenticated (Paragraphs 73-78; showing that if any of the verification steps, including authentication of the digital signature, fail, the process will abort and the data will not be used). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the content authentication and access control system of Collins into the content usage control system of Uranaka as modified by Tsumagari in order to allow the system to detect when

errors in the data have occurred, such that data with errors will not be allowed to be processed and only correct data will be processed, and/or to ensure that the data is authentic before allowing access to proceed, thereby increasing security of the system by ensuring both integrity and authenticity of the content.

Regarding Claim 28,

Uranaka as modified by Tsumagari and Collins discloses the method of claim 27, in addition, Uranaka discloses that the coordination between the read out media and downloaded content will be established if the downloaded content is authenticated (Column 15, lines 57-67); and Collins discloses allowing use of downloaded content if the downloaded content is authenticated (Paragraphs 73-77).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be

calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner

Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437